REMARKS

Claims 2 to 6, 12 and 14 are pending in the present application, of which claims 2, 12 and 14 are independent. No amendments have been made. Applicants believe that the present application is in condition for allowance and request the Examiner to reconsider the rejection in light of the remarks set forth below.

REJECTION UNDER 35 U.S.C. §102

The Examiner rejected claims 1 to 6, 12 and 14 under 35 U.S.C. §102(e) as being allegedly anticipated by U.S. Patent No. 6,151,676 issued to Cuccia et al. (hereinafter "Cuccia"). The rejection is respectfully traversed in its entirety.

> To anticipate a claim under 35 U.S.C. §102(e), the reference must teach every element of the claim and "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (see MPEP §2131).

Cuccia discusses digital signatures signed using the El-Gamal algorithm (col. 5, lines 48 to 56). It teaches using user identifying keys to secure private keys for users, wherein the ucr identifying keys are derived from user identifying information obtained by interaction with the user physically present at the user equipment (col. 5, lines 63 to 67). Cuccia also discusses the use of secret random numbers and a freshness value in the encryption, decryption, signature and verification operations (col. 7, line 66 to col. 8, line 12 and col. 8, lines 33 to 59). The random numbers prevent an attacker from discovering the user's private key from a signature while the freshness value assures the freshness of the encrypted random numbers (col. 9, line 63 to col. 10, line 14).

In the Office Action, the Examiner equates the above secret random numbers of Cuccia to the crypto-sync value of claims 2, 12 and 14. Applicants respectfully disagree. Cuccia teaches generating the random number based on a natural random phenomenon (col. 9, lines 6 to

2

8). Accordingly, incrementing the random numbers would not possible and is not disclosed or even suggested. Therefore, Cuccia does not disclose or teach incrementing a crypto-sync value as in independent claims 2, 12 and 14.

Moreover, claims 3 to 6 depend from and include all the elements cited in the independent claim 2. Accordingly, Applicants submit that these claims are believed to be allowable based on their dependency from an allowable base claim as well as other novel features included therein.

In particular, assuming for the purposes of argument that the random numbers of Cuccia can be equated to the crypto-sync value, there is no teaching in Cuccia of generating the random numbers using a sequence number value, data unit identification number, a system time value or a directional bit as in claims 3 and 4, respectively. Note here that the freshness value may be generated using a system time.

For at least the foregoing reasons, Applicants respectfully submit that Cuccia does not teach every element of the claims and request a withdrawal of the rejection under 35 U.S.C. §102.

3

Attorney Docket No. 990594

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: April 5 , 2005   By: _____

Jae-Hee Choi, Reg. No. 45,288
(858)651-5469

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

4